Protecting Against Data Breaches

The possibility of the average consumer becoming a victim of a data breach grows with each new advancement in electronics. A data breach occurs when sensitive or confidential information—driver's license numbers, medical records, Social Security numbers, bank or credit card account numbers—is stolen, copied or used by an unauthorized person.

In 2004, only one state required businesses to alert consumers if their personal data had been stolen. Since then, legislation has passed in 45 additional states, including Indiana, to ensure that affected consumers are contacted should their personal information be lost or stolen.

While news spreads quickly when there is a major breach affecting millions of accounts, large companies are not the only ones that suffer from such thefts. Smaller companies can be compromised by an employee, a partner or an external computer hacker.

Prevention

Consumers can take the following steps to protect against a personal data breach:

- Review credit card and bank statements for fraudulent charges at least once a month. If there is a suspicious charge, contact your financial institution.
- Request that your financial institution close any accounts that you suspect were compromised, and ask for replacement cards with new account numbers and PINs.
- Determine if there have been unusual requests, such as change-of-address or attempts to secure additional or replacement credit cards.
- Instruct the card issuer not to honor any requests regarding your card without your written authorization.
- Credit card issuers offer a variety of e-mail and/or text notices. You can ask for a notice when charges over a certain amount are made, or when your balance reaches a certain level.

Follow Up

If you have been the victim of identity theft, contact the three credit reporting agencies—Equifax, Experian and TransUnion—to place a security freeze on your account:

- Equifax 800-525-6285, www.equifax.com
- Experian 888-397-3742, www.experian.com
- TransUnion 800-680-7289, www.transunion.com

Report the identity theft to the police, as you may need to provide a copy of the police report to your bank, creditors and credit reporting agencies. If the local police are not familiar with investigating information compromises, contact the local office of the FBI or the U.S. Secret Service.

To ensure that an identity thief has not opened a new account in your name, you should review your credit report. To obtain a free copy of the report, go to www.annualcreditreport.com. If there are any accounts on your report that you did not open, contact the credit bureau to report the fraud and dispute the charges.

Provided as a public service by the Indiana Bankers Association.

IBA INDIANA BANKERS ASSOCIATION